

IN THE UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF VIRGINIA

IN THE MATTER OF THE SEARCH OF T-MOBILE CELLULAR PHONE WITH SUSCRIBER NUMBER OF (347) 513-7635 CURRENTLY LOCATED IN FBI EVIDENCE LOCKER, LOCATED AT 210 FRANKLIN RD SW, ROANOKE, VA 24011.

Case No. 7:22mj69

AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE

I, Jason McCoy, being duly sworn, state the following is true and correct to the best of my knowledge and belief:

INTRODUCTION, AGENT BACKGROUND, AND PURPOSE OF THE WARRANT

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and extraction from this device of electronically stored information as described in Attachment B.

2. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that NAJALAEK WALKER (hereafter referred to as WALKER) violated Title 18 U.S.C § 922(g), 18 U.S.C § 924(c), and 21 U.S.C § 841(a)(1), which make it a crime to possess with the intent to distribute certain controlled substances, to possess a firearm as a prohibited person, and to possess one or more firearms in furtherance of drug trafficking.

3. There is also probable cause to search this electronic device for evidence, instrumentalities, contraband, and/or fruits of these crimes, as further described in Attachment B.

4. The facts in this affidavit come from my personal observations, my training and experience, information from records and databases, and information obtained from other agents and witnesses. This affidavit does not set forth all of my knowledge about this matter; it is intended to only show that there is sufficient probable cause for the requested warrant. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only. All dates, times, and ages are approximate.

5. I am a Special Agent with the Federal Bureau of Investigation (FBI) assigned to the Richmond, Virginia, Field Office, Lynchburg Resident Agency. I have been employed with the FBI since July 2019 and as a law enforcement officer since 2007. Prior to joining the FBI, I was a Special Agent with the United States Air Force Office of Special Investigations and began conducting federal criminal investigations after completing the Federal Law Enforcement Training Center's (FLETC) Criminal Investigator Training Program (CITP) in September 2013. As part of my duties, I investigate criminal violations relating to firearms violations and drug offenses under titles 18 and 21 of the United States Code. I am presently and have been previously assigned to investigate a variety of criminal matters, to include violent criminal acts. Further, I have experience and training in a variety of investigative and legal matters, including the topics of lawful arrests, drafting of search warrant affidavits, and probable cause. While serving within my capacity at the FBI, I have authored search warrants concerning various federal criminal violations. I have investigated cases where electronic communications to include social media platforms and cellular telephones have played an integral role in the investigations.

Through experience and training received, I have become familiar with how the usage of electronic devices and social media applications have become commonplace throughout the “criminal world.” I have also become aware that information stored at the service provider facilities and on cellular devices themselves can assist law enforcement in criminal investigations.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

6. The electronic device to be searched is a T-Mobile cellular phone with subscriber number (347) 513-7635 (hereinafter, the “Device”). The Device is currently secured in the FBI evidence locker located at 210 Franklin Road, SW, Roanoke, VA 24011.

7. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data as described in Attachment B.

FACTUAL BACKGROUND OF INVESTIGATION AND PROBABLE CAUSE

8. On November 27, 2021, personnel from the FBI and Lynchburg Police Department (LPD) were requested to assist with the arrest of NAJALAEK WALKER in the Western District of Virginia. In relation to this request, the officers were notified that WALKER had an extraditable warrant issued by the state of New York for a parole violation, and was traveling on Greyhound bus #1151, scheduled to stop in Lynchburg, Virginia at approximately 11:30 AM that morning. Law enforcement personnel coordinated an arrest operation in Lynchburg based on this information.

9. When bus #1151 arrived at the appointed Lynchburg station, officers identified WALKER from a photograph and arrested him. He was carrying what appeared to be a fast food

container as he stepped off the bus, which he dropped as officers were taking him into physical custody. A 9mm pistol fell from the food container and was immediately secured by law enforcement. The pistol had one round of ammunition in the chamber and an additional 11 rounds of ammunition in the magazine. During a search of his person incident to arrest, WALKER was also found to be in possession of a quantity of suspected narcotics, a clear plastic bag containing eight additional rounds of ammunition, as well as the Device. The suspected narcotics were in a clear plastic bag containing multiple smaller individual bags of white powdery substances and one containing a brown powdery substance, which since have lab-tested positively for the presence of cocaine, heroin, and/or fentanyl. The total weight of the suspected cocaine was approximately eight grams before testing. The total weight of the suspected heroine was approximately one and a half (1.5) grams before testing.

10. Based on the warrant issued for violating conditions of his parole, WALKER was taken into custody by the LPD and booked into the Blue Ridge Regional Jail, located in Lynchburg, Virginia. Law enforcement seized the 9mm pistol, suspected narcotics, and the Device.

11. Investigators from New York assumed custody of the Device in Lynchburg on November 27, 2021. The FBI has maintained custody of the Device in New York since then for use in a separate investigation, and obtained a warrant to search its contents. Custody of the Device was transferred to law enforcement personnel in the Western District of Virginia for use in this case on June 27, 2022. Your undersigned affiant returned to this district from military leave on July 5, 2022, prompting the instant request for a warrant to search the Device for evidence of the crimes at issue in this case. On information and belief, WALKER has made no request for the return of the Device.

TECHNICAL TERMS

12. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by

connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special

sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments, or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.
- f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal

computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

- g. Pager: A pager is a handheld wireless electronic device used to contact an individual through an alert, or a numeric or text message sent over a telecommunications network. Some pagers enable the user to send, as well as receive, text messages.
- h. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- i. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

13. Based on my training, experience, and research, I know that drug traffickers will often carry and use electronic devices such as wireless telephones to communicate with third parties about their illicit transactions, including communications about drugs and firearms. Their devices will frequently contain evidence of these communications in text, data or image form. From my training, experience, and research, I know the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. Additionally, the Device can be utilized to access the internet. As a result, examining data stored on the Device may uncover, among other things, evidence that reveals or suggests who possessed or used the Device, specific communications between users of the Device and/or third parties pertaining to the crimes under investigation, and pertinent data and other information downloaded to or accessed through the Device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

14. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

15. There is probable cause to believe things that were once stored on the Device may still be stored there, for at least the following reasons:

- j. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet.

Electronic files downloaded to a storage medium can be stored for years at little

or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- k. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- l. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- m. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

16. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- n. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.
- o. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- p. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw

conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

- q. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- r. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

17. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

18. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve

the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

19. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

REQUEST FOR SEALING

20. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the internet and disseminate them to other online criminals as they deem appropriate, i.e., by posting them publicly online through various forums. In addition, if alerted to the existence of this warrant, WALKER or his associates may be able to interfere remotely with attempts by law enforcement to secure information from the Device. Premature disclosure of the contents of this affidavit and related documents may therefore jeopardize the effectiveness of this aspect of the investigation.

Respectfully submitted,

JASON MCCOY Digitally signed by JASON MCCOY
Date: 2022.07.06 14:39:55 -04'00'

Jason P. McCoy
Special Agent, Federal Bureau of Investigation

Subscribed and sworn to before me
on July 6, 2022:

Robert S. Ballou

Honorable Robert S. Ballou
UNITED STATES MAGISTRATE JUDGE